

**Roth's Theorem: If  $A \subseteq [n]$  is large then it has a 3-AP**  
**Roth's Proof**  
 by **William Gasarch (gasarch@cs.umd.edu)**

## 1 Roth's Theorem

**Notation 1.1** Let  $[n] = \{1, \dots, n\}$ . If  $k \in \mathbf{N}$  then  $k$ -AP means an arithmetic progression of size  $k$ .

Consider the following statement:

If  $A \subseteq [n]$  and  $\#(A)$  is 'big' then  $A$  must have a 3-AP.

This statement, made rigorous, is true. In particular, the following is true and easy:

Let  $n \geq 3$ . If  $A \subseteq [n]$  and  $\#(A) \geq 0.7n$  then  $A$  must have a 3-AP.

Can we lower the constant 0.7? We can lower it as far as we like if we allow  $n$  to start later:

Roth [3, 4, 5] proved the following using analytic means.

$(\forall \lambda > 0)(\exists n_0 \in \mathbf{N})(\forall n \geq n_0)(\forall A \subseteq [n])(\#(A) \geq \lambda n \Rightarrow A \text{ has a 3-AP})$ .

The analogous theorem for 4-APs was later proven by Szemerédi [3, 6] by a combinatorial proof. Szemerédi [7] later (with a much harder proof) generalized from 4 to any  $k$ .

We prove the  $k = 3$  case using the analytic techniques of Roth; however, we rely heavily on Gowers [2, 1]

**Definition 1.2** Let  $sz(n)$  be the least number such that, for all  $A \subseteq [n]$ , if  $\#(A) \geq sz(n)$  then  $A$  has a 3-AP. Note that if  $A \subseteq [a, a + n - 1]$  and  $\#(A) \geq sz(n)$  then  $A$  has a 3-AP. Note also that if  $A \subseteq \{a, 2a, 3a, \dots, na\}$  and  $\#(A) \geq sz(n)$  then  $A$  has a 3-AP. More generally, if  $A$  is a subset of any equally spaced set of size  $n$ , and  $\#(A) \geq sz(n)$ , then  $A$  has a 3-AP.

## 2 Sparse Intervals

The next lemma states that if  $A$  is 'big' and 3-free then it is somewhat uniform. There cannot be sparse intervals of  $A$ . The intuition is that if  $A$  has a sparse interval then the rest of  $A$  has to be dense to make up for it, and it might have to be so dense that it has a 3-AP.

**Lemma 2.1** Let  $n, n_0 \in \mathbf{N}; \lambda, \lambda_0 \in (0, 1)$ . Assume  $\lambda < \lambda_0$  and  $(\forall m \geq n_0)[sz(m) \leq \lambda_0 m]$ . Let  $A \subseteq [n]$  be a 3-free set such that  $\#(A) \geq \lambda n$ . Let  $a, b$  be such that  $a < b$ ,  $a > n_0$ , and  $n - b > n_0$ . Then  $\lambda_0(b - a) - n(\lambda_0 - \lambda) \leq \#(A \cap [a, b])$ .

**Proof:**

Since  $A$  is 3-free and  $a \geq n_0$  and  $n - b \geq n_0$  we have  $\#(A \cap [1, a - 1]) < \lambda_0(a - 1) < \lambda_0 a$  and  $\#(A \cap [b + 1, n]) < \lambda_0(n - b)$ . Hence

$$\begin{aligned} \lambda n \leq \#(A) &= \#(A \cap [1, a - 1]) + \#(A \cap [a, b]) + \#(A \cap [b + 1, n]) \\ \lambda n &\leq \lambda_0 a + \#(A \cap [a, b]) + \lambda_0(n - b) \\ \lambda n - \lambda_0 n + \lambda_0 b - \lambda_0 a &\leq \#(A \cap [a, b]) \\ \lambda_0(b - a) - n(\lambda_0 - \lambda) &\leq \#(A \cap [a, b]). \end{aligned}$$

■

### 3 Notation

Throughout this paper the following hold.

1.  $n \in \mathbb{N}$  is a fixed large prime.
2.  $\mathbb{Z}_n = \{1, \dots, n\}$  with modular arithmetic.
3.  $\omega = e^{2\pi i/n}$ .
4. If  $a$  is a complex number then  $|a|$  is its length.
5. If  $A$  is a set then  $|A|$  is its cardinality.

### 4 Counting 3-AP's

**Lemma 4.1** *Let  $A, B, C \subseteq [n]$ . The number of  $(x, y, z) \in A \times B \times C$  such that  $x + z \equiv 2y \pmod{n}$  is*

$$\frac{1}{n} \sum_{x, y, z \in [n]} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)}.$$

**Proof:**

We break the sum into two parts:

Part 1:

$$\frac{1}{n} \sum_{x, y, z \in [n], x+z \equiv 2y \pmod{n}} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)}.$$

Note that we can replace  $\omega^{-r(x-2y+z)}$  with  $\omega^0 = 1$ . We can then replace  $\sum_{r=1}^n 1$  with  $n$ . Hence we have

$$\frac{1}{n} \sum_{x, y, z \in [n], x+z \equiv 2y \pmod{n}} A(x)B(y)C(z)n = \sum_{x, y, z \in [n], x+z \equiv 2y \pmod{n}} A(x)B(y)C(z)$$

This is the number of  $(x, y, z) \in A \times B \times C$  such that  $x + z \equiv 2y \pmod{n}$ .

Part 2:

$$\frac{1}{n} \sum_{x, y, z \in [n], x+z \not\equiv 2y \pmod{n}} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)}.$$

We break this sum up depending on what the (nonzero) value of  $w = x + z - 2y \pmod{n}$ . Let

$$S_u = \sum_{x, y, z \in [n], x-2y+z=2} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-ru}.$$

Since  $u \neq 0$ ,  $\sum_{r=1}^n \omega^{-ru} = \sum_{r=1}^n \omega^{-r} = 0$ . Hence  $S_u = 0$ .

Note that

$$\frac{1}{n} \sum_{x,y,z \in [n], x+z \not\equiv 2y \pmod{n}} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} = \frac{1}{n} \sum_{u=1}^{n-1} S_u = 0$$

The lemma follows from Part 1 and Part 2.  $\blacksquare$

**Lemma 4.2** *Let  $A \subseteq [n]$ . Let  $B = C = A \cap [n/3, 2n/3]$ . The number of  $(x, y, z) \in A \times B \times C$  such that  $x, y, z$  forms a 3-AP is at least*

$$\frac{1}{2n} \sum_{x,y,z \in [n]} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} - O(n).$$

**Proof:** By Lemma 4.1

$$\frac{1}{n} \sum_{x,y,z \in [n]} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)}$$

is the number of  $(x, y, z) \in A \times B \times C$  such that  $x + z \equiv 2y \pmod{n}$ . This counts three types of triples:

- Those that have  $x = y = z$ . There are  $n/3$  of them.
- Those that have  $x + z = 2y + n$ . There are  $O(1)$  of them.
- Those that have  $x \neq y, y \neq z, x \neq z$ , and  $x + z = 2y$ .

Hence

$$\#\{(x, y, z) : (x+z = 2y) \wedge x \neq y \wedge y \neq z \wedge x \neq z\} = \frac{1}{n} \sum_{x,y,z \in [n]} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} - O(n).$$

We are not done yet. Note that  $(5, 10, 15)$  may show up as  $(15, 10, 5)$ . Every triple appears at most twice. Hence

$$\begin{aligned} & \#\{(x, y, z) : (x + z = 2y) \wedge x \neq y \wedge y \neq z \wedge x \neq z\} \\ & \leq 2\#\{(x, y, z) : (x < y < z) \wedge (x + z = 2y) \wedge x \neq y \wedge y \neq z \wedge x \neq z\}. \end{aligned}$$

Therefore

$$\frac{1}{2n} \sum_{x,y,z \in [n]} A(x)B(y)C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} - O(n) \leq \text{the number of 3-AP's with } x \in A, y \in B, z \in C.$$

$\blacksquare$

We will need to re-express this sum. For that we will use Fourier Analysis.

## 5 Fourier Analysis

**Definition 5.1** If  $f : Z_n \rightarrow \mathbb{N}$  then  $\hat{f} : Z_n \rightarrow \mathbb{C}$  is

$$\hat{f}(r) = \sum_{s \in [n]} f(s)\omega^{-rs}.$$

$\hat{f}$  is called the *Fourier Transform* of  $f$ .

What does  $\hat{f}$  tell us? We look at the case where  $f$  is the characteristic function of a set  $A \subseteq [n]$ . Henceforth we will use  $A(x)$  instead of  $f(x)$ .

We will need the following facts.

**Lemma 5.2** Let  $A \subseteq \{1, \dots, n\}$ .

1.  $\hat{A}(n) = \#(A)$ .
2.  $\max_{r \in [n]} |\hat{A}(r)| = \#(A)$ .
3.  $A(s) = \frac{1}{n} \sum_{r=1}^n \hat{A}(r)\omega^{-rs}$ . *DO WE NEED THIS?*
4.  $\sum_{r=1}^n |\hat{A}(r)|^2 = n\#(A)$ .
5.  $\sum_{s=1}^n A(s) = \frac{1}{n} \sum_{r=1}^n \hat{A}(r)$ .

**Proof:**

Note that  $\omega^n = 1$ . Hence

$$\hat{A}(n) = \sum_{s \in [n]} A(s)\omega^{-ns} = \sum_{s \in [n]} A(s) = \#(A).$$

Also note that

$$|\hat{A}(r)| = \left| \sum_{s \in [n]} A(s)\omega^{-rs} \right| \leq \sum_{s \in [n]} |A(s)\omega^{-rs}| \leq \sum_{s \in [n]} |A(s)| |\omega^{-rs}| \leq \sum_{s \in [n]} |A(s)| = \#(A).$$

■

**Informal Claim:** If  $\hat{A}(r)$  is large then there is an arithmetic sequence  $P$  with difference  $r^{-1} \pmod{n}$  such that  $\#(A \cap P)$  is large.

We need a lemma before we can prove the claim.

**Lemma 5.3** Let  $n, m \in \mathbb{N}$ ,  $s_1, \dots, s_m$ , and  $0 < \lambda, \alpha, \epsilon < 1$  be given (no order on  $\lambda, \alpha, \epsilon$  is implied). Assume that  $(\lambda - \frac{m-1}{m}(\lambda + \epsilon)) \geq 0$ . Let  $f(x_1, \dots, x_m) = |\sum_{j=1}^m x_j \omega^{s_j}|$ . The maximum value that  $f(x_1, \dots, x_m)$  can achieve subject to the following two constraints (1)  $\sum_{j=1}^m x_j \geq \lambda n$ , and (2)  $(\forall j)[0 \leq x_j \leq (\lambda + \epsilon)\frac{n}{m}]$  is bounded above by  $\epsilon mn + (\lambda + \epsilon)\frac{n}{m} |\sum_{j=1}^m \omega^{s_j}|$

**Proof:**

Assume that the maximum value of  $f$ , subject to the constraints, is achieved at  $(x_1, \dots, x_m)$ . Let  $MIN$  be the minimum value that any variable  $x_i$  takes on (there may be several variables that take this value). What is the smallest that  $MIN$  could be? By the constraints this would occur when all but one of the variables is  $(\lambda + \epsilon)\frac{n}{m}$  and the remaining variable has value  $MIN$ . Since  $\sum x_i \geq \lambda n$  we have

$$MIN + (m-1)(\lambda + \epsilon)\frac{n}{m} \geq \lambda n$$

$$MIN + \frac{m-1}{m}(\lambda + \epsilon)n \geq \lambda n$$

$$MIN \geq \lambda n - \frac{m-1}{m}(\lambda + \epsilon)n$$

$$MIN \geq (\lambda - \frac{m-1}{m}(\lambda + \epsilon))n$$

Hence note that, for all  $j$ ,

$$x_j - MIN \leq x_j - (\lambda - \frac{m-1}{m}(\lambda + \epsilon))n$$

Using the bound on  $x_j$  from constraint (2) we obtain

$$\begin{aligned} x_j - MIN &\leq (\lambda + \epsilon)\frac{n}{m} - (\lambda - \frac{m-1}{m}(\lambda + \epsilon))n \\ &\leq ((\lambda + \epsilon)\frac{1}{m} - (\lambda - \frac{m-1}{m}(\lambda + \epsilon)))n \\ &\leq ((\lambda + \epsilon)\frac{1}{m} - \lambda + \frac{m-1}{m}(\lambda + \epsilon))n \\ &\leq \epsilon n \end{aligned}$$

Note that

$$\begin{aligned} |\sum_{j=1}^m x_j \omega^{sj}| &= |\sum_{j=1}^m (x_j - MIN)\omega^{sj} + \sum_{j=1}^m MIN\omega^{sj}| \\ &\leq |\sum_{j=1}^m (x_j - MIN)\omega^{sj}| + |\sum_{j=1}^m MIN\omega^{sj}| \\ &\leq \sum_{j=1}^m |(x_j - MIN)| |\omega^{sj}| + MIN |\sum_{j=1}^m \omega^{sj}| \\ &\leq \sum_{j=1}^m \epsilon n + MIN |\sum_{j=1}^m \omega^{sj}| \\ &\leq \epsilon mn + MIN |\sum_{j=1}^m \omega^{sj}| \\ &\leq \epsilon mn + (\lambda + \epsilon)\frac{n}{m} |\sum_{j=1}^m \omega^{sj}| \end{aligned}$$

■

**Lemma 5.4** *Let  $A \subseteq [n]$ ,  $r \in [n]$ , and  $0 < \alpha < 1$ . If  $|\hat{A}(r)| \geq \alpha n$  and  $|A| \geq \lambda n$  then there exists  $m \in \mathbb{N}$ ,  $0 < \epsilon < 1$ , and an arithmetic sequence  $P$  within  $\mathbb{Z}_n$ , of length  $\frac{n}{m} \pm O(1)$  such that  $\#(A \cap P) \geq (\lambda + \epsilon)\frac{n}{m}$ . The parameters  $\epsilon$  and  $m$  will depend on  $\lambda$  and  $\alpha$  but not  $n$ .*

**Proof:** Let  $m$  and  $\epsilon$  be parameters to be picked later. We will note constraints on them as we go along. (Note that  $\epsilon$  will not be used for a while.)

Let  $1 = a_1 < a_2 < \dots < a_{m+1} = n$  be picked so that

$a_2 - a_1 = a_3 - a_2 = \dots = a_m - a_{m-1}$  and  $a_{m+1} - a_m$  is as close to  $a_2 - a_1$  as possible.

For  $1 \leq j \leq m$  let

$$P_j = \{s \in [n] : a_j \leq rs \pmod{n} < a_{j+1}\}.$$

Let us look at the elements of  $P_j$ . Let  $r^{-1}$  be the inverse of  $r \pmod{n}$ .

1.  $s$  such that  $a_j \equiv rs \pmod{n}$ , that is,  $s \equiv a_j r^{-1} \pmod{n}$ .
2.  $s$  such that  $a_j + 1 \equiv rs \pmod{n}$ , that is  $s \equiv (a_j + 1)r^{-1} \equiv a_j r^{-1} + r^{-1} \pmod{n}$ .

3.  $s$  such that  $a_j + 2 \equiv rs \pmod{n}$ , that is  $s \equiv (a_j + 2)r^{-1} \equiv a_j r^{-1} + 2r^{-1} \pmod{n}$ .

4.  $\vdots$

Hence  $P_j$  is an arithmetic sequence within  $\mathbb{Z}_n$  which has difference  $r^{-1}$ . Also note that  $P_1, \dots, P_m$  form a partition of  $\mathbb{Z}_n$  into  $m$  parts of size  $\frac{n}{m} + O(1)$  each.

Recall that

$$\hat{A}(r) = \sum_{s \in [n]} A(s) \omega^{-rs}.$$

Lets look at  $s \in P_j$ . We have that  $a_j \leq rs \pmod{n} < a_{j+1}$ . Therefore the values of  $\{\omega^{rs} : s \in P_j\}$  are all very close together. We will pick  $s_j \in P_j$  carefully. In particular we will constrain  $m$  so that it is possible to pick  $s_j \in P_j$  such that  $\sum_{j=1}^m \omega^{-rs_j} = 0$ . For  $s \in P_j$  we will approximate  $\omega^{-rs}$  by  $\omega^{-rs_j}$ . We skip the details of how good the approximation is.

We break up the sum over  $s$  via  $P_j$ .

$$\begin{aligned} \hat{A}(r) &= \sum_{s \in [n]} A(s) \omega^{-rs} \\ &= \sum_{j=1}^m \sum_{s \in P_j} A(s) \omega^{-rs} \\ &\sim \sum_{j=1}^m \sum_{s \in P_j} A(s) \omega^{-rs_j} \\ &= \sum_{j=1}^m \omega^{-rs_j} \sum_{s \in P_j} A(s) \\ &= \sum_{j=1}^m \omega^{-rs_j} \#(A \cap P_j) \\ &= \sum_{j=1}^m \#(A \cap P_j) \omega^{-rs_j} \\ \alpha n \leq |\hat{A}(r)| &= \left| \sum_{j=1}^m \#(A \cap P_j) \omega^{-rs_j} \right| \end{aligned}$$

We will not use  $\epsilon$ . We intend to use Lemma 5.3; therefore we have the constraint  $(\lambda - \frac{m-1}{m}(\lambda + \epsilon)) \geq 0$ .

Assume, by way of contradiction, that  $(\forall j)[|A \cap P_j| \leq (\lambda + \epsilon) \frac{n}{m}]$ . Applying Lemma 5.3 we obtain

$$\left| \sum_{j=1}^m \#(A \cap P_j) \omega^{-rs_j} \right| \leq \epsilon m n + (\lambda + \epsilon) \frac{n}{m} \left| \sum_{j=1}^m \omega^{-rs_j} \right| = \epsilon m n.$$

Hence we have

$$\alpha n \leq \epsilon m n$$

$$\alpha \leq \epsilon m.$$

In order to get a contradiction we pick  $\epsilon$  and  $m$  such that  $\alpha > \epsilon m$ .

Having done that we now have that  $(\exists j)[|A \cap P_j| \geq (\lambda + \epsilon) \frac{n}{m}]$ .

We now list all of the constraints introduced and say how to satisfy them.

1.  $m$  is such that there exists  $s_1 \in P_1, \dots, s_m \in P_m$  such that  $\sum_{j=1}^m \omega^{-rs_j} = 0$ , and
2.  $(\lambda - \frac{m-1}{m}(\lambda + \epsilon)) \geq 0$ .
3.  $\epsilon m < \alpha$ .

First pick  $m$  to satisfy item 1. Then pick  $\epsilon$  small enough to satisfy items 2,3.  $\blacksquare$

**Lemma 5.5** *Let  $A, B, C \subseteq [n]$ . The number of 3-AP's  $(x, y, z) \in A \times B \times C$  is bounded below by*

$$\frac{1}{2n} \sum_{r=1}^n \hat{A}(r) \hat{B}(-2r) \hat{C}(r) - O(n).$$

**Proof:**

The number of 3-AP's is bounded below by

$$\frac{1}{2n} \sum_{x, y, z \in [n]} A(x) B(y) C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} - O(n) =$$

We look at the inner sum.

$$\begin{aligned} & \sum_{x, y, z \in [n]} A(x) B(y) C(z) \sum_{r=1}^n \omega^{-r(x-2y+z)} = \\ & \sum_{r=1}^n \sum_{x, y, z \in [n]} A(x) \omega^{-rx} B(y) \omega^{2yr} C(z) \omega^{-rz} = \\ & \sum_{r=1}^n \sum_{x \in [n]} A(x) \omega^{-rx} \sum_{y \in [n]} B(y) \omega^{2yr} \sum_{z \in \mathbb{Z}_r} C(z) \omega^{-rz} = \\ & \sum_{r=1}^n \hat{A}(r) \hat{B}(-2r) \hat{C}(r). \end{aligned}$$

The Lemma follows.  $\blacksquare$

## 6 Main Theorem

**Theorem 6.1** *For all  $\lambda$ ,  $0 < \lambda < 1$ , there exists  $n_0 \in \mathbb{N}$  such that for all  $n \geq n_0$ ,  $sz(n) \leq \lambda n$ .*

**Proof:**

Let  $S(\lambda)$  be the statement

*there exists  $n_0$  such that, for all  $n \geq n_0$ ,  $sz(n) \leq \lambda n$ .*

It is a trivial exercise to show that  $S(0.7)$  is true.

Let

$$C = \{\lambda : S(\lambda)\}.$$

$C$  is closed upwards. Since  $0.7 \in C$  we know  $C \neq \emptyset$ . Assume, by way of contradiction, that  $C \neq (0, 1)$ . Then there exists  $\lambda < \lambda_0$  such that  $\lambda \notin C$  and  $\lambda_0 \in C$ . We can take  $\lambda_0 - \lambda$  to be as small as we like. Let  $n_0$  be such that  $S(\lambda_0)$  is true via  $n_0$ . Let  $n \geq n_0$  and let  $A \subseteq [n]$  such that  $\#(A) \geq \lambda n$  but  $A$  is 3-free.

Let  $B = C = A \cap [n/3, 2n/3]$ .

By Lemma 5.5 the number of 3-AP's of  $A$  is bounded below by

$$\frac{1}{2n} \sum_{r=1}^n \hat{A}(r) \hat{B}(-2r) \hat{C}(r) - O(n).$$

We will show that either this is positive or there exists a set  $P \subseteq [n]$  that is an AP of length  $\text{XXX}$  and has density larger than  $\lambda$ . Hence  $P$  will have a 3-AP.

By Lemma 5.2 we have  $\hat{A}(n) = \#(A)$ ,  $\hat{B}(n) = \#(B)$ , and  $\hat{C}(n) = \#(C)$ . Hence

$$\begin{aligned} & \frac{1}{2n} \hat{A}(n) \hat{B}(n) \hat{C}(n) + \frac{1}{2n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r) - O(n) = \\ & \frac{1}{2n} \#(A) \#(B) \#(C) + \frac{1}{2n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r) - O(n). \end{aligned}$$

By Lemma 2.1 we can take  $\#(B), \#(C) \geq n\lambda/4$ . We already have  $\#(A) \geq \lambda n$ . This makes the lead term  $\Omega(n^3)$ ; hence we can omit the  $O(n)$  term. More precisely we have that the number of 3-AP's in  $A$  is bounded below by

$$\frac{\lambda^3 n^2}{32} + \frac{1}{2n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r).$$

We are assuming that this quantity is  $\leq 0$ .

$$\frac{\lambda^3 n^2}{32} + \frac{1}{2n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r) < 0.$$

$$\frac{\lambda^3 n^2}{16} + \frac{1}{n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r) < 0.$$

$$\frac{\lambda^3 n^2}{16} < -\frac{1}{n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r).$$

Since the left hand side is positive we have

$$\begin{aligned} \frac{\lambda^3 n^2}{16} & < \left| \frac{1}{n} \sum_{r=1}^{n-1} \hat{A}(r) \hat{B}(-2r) \hat{C}(r) \right| \\ & < \frac{1}{n} (\max_r \hat{A}(r)) \sum_{r=1}^{n-1} |\hat{B}(-2r)| |\hat{C}(r)| \end{aligned}$$

By the Cauchy Schwartz inequality we know that

$$\sum_{i=1}^{n-1} |\hat{B}(-2r)| |\hat{C}(r)| \leq \left( \sum_{i=1}^{n-1} |\hat{B}(-2r)|^2 \right)^{1/2} \left( \sum_{i=1}^{n-1} |\hat{C}(r)|^2 \right)^{1/2}.$$

Hence

$$\frac{\lambda^3 n^2}{16} < \frac{1}{n} \max_{1 \leq r \leq n-1} |\hat{A}(r)| \left( \sum_{i=1}^{n-1} |\hat{B}(-2r)|^2 \right)^{1/2} \left( \sum_{i=1}^{n-1} |\hat{C}(r)|^2 \right)^{1/2}.$$

By Parsaval's inequality and the definition of  $B$  and  $C$  we have

$$\sum_{i=1}^{n-1} |\hat{B}(-2r)|^2)^{1/2} \leq n\#(B) = \frac{\lambda n^2}{3}$$

and

$$\sum_{i=1}^{n-1} |\hat{C}(r)|^2)^{1/2} \leq n\#(C) = \frac{\lambda n^2}{3}$$

Hence

$$\frac{\lambda^3 n^2}{16} < \left( \max_{1 \leq r \leq n-1} |\hat{A}(r)| \right) \frac{1}{n} \frac{\lambda n^2}{3} = \left( \max_{1 \leq r \leq n-1} |\hat{A}(r)| \right) \frac{\lambda n}{3}.$$

Therefore

$$|\hat{A}(r)| \geq \frac{3\lambda^2 n}{16}. \quad \blacksquare$$

## References

- [1] W. Gowers. A new proof for Szemerédi's theorem for arithmetic progressions of length four. *Geometric and Functional Analysis*, 8:529–551, 1998.
- [2] W. Gowers. A new proof of Szemerédi's theorem. *Geometric and Functional Analysis*, 11:465–588, 2001. Available at <http://www.dpmms.cam.ac.uk/~wtg10/papers/html>.
- [3] R. Graham, A. Rothchild, and J. Spencer. *Ramsey Theory*. Wiley, 1990.
- [4] K. Roth. Sur quelques ensembles d'entiers. *C.R. Acad. Sci Paris*, 234:388–3901, 1952.
- [5] K. Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 28:104–109, 1953.
- [6] E. Szemerédi. On sets of integers containing no four elements in arithmetic progression. *Acta Math. Sci. Hung.*, 20:89–104, 1969.
- [7] E. Szemerédi. On sets of integers containing no  $k$  elements in arithmetic progression. *Acta Arith.*, 27:299–345, 1986.